NORGE

(12) **PATENT**

(19) NO (11) **313810** (13) B1

(51) Int Cl[7] H 04 L 9/32, 9/00, H 04 Q 7/32

Patentstyret

(21) Søknadsnr	20012030	(86) Int. inng. dag og søknadsnummer	
(22) Inng. dag	2001.04.25		
(24) Løpedag	2001.04.25	(85) Videreføringsdag	
(41) Alm. tilgj.	2002.10.28	(30) Prioritet	Ingen
(45) Meddelt dato	2002.12.02		

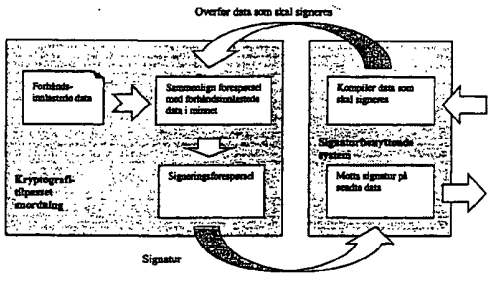
(71) Patenthaver Telefonaktiebolaget L M Ericsson, S-126 25 Stockholm, SE
(72) Oppfinner Sverre Tønnesland, 0659 Oslo, NO
Pål Bjølseth, 0276 Oslo, NO
(74) Fullmektig Oslo Patentkontor AS, 0306 Oslo

(54) Benevnelse **Kryptografisk signering i små enheter**

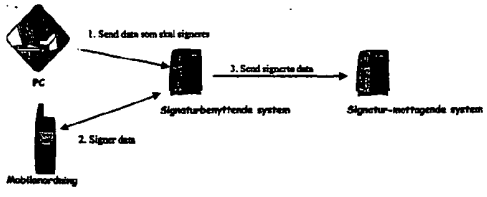
(56) Anførte publikasjoner WML Script Crypto Library fra http://www.wapforum.org/tech/documents...
WO 0039958

(57) Sammendrag

Fremgangsmåte for elektronisk og/eller digital signering av data på en liten signeringsanordning for eksempel en mobiltelefon, er angitt. Fremgangsmåten omfatter en sammenligning av data som skal signeres med et eller flere sett med attributter forhåndslagret på signeringsanordningen og å vise attributtene på nevnte signeringsanordning hvis nevnte data matcher alle, en del av eller deler av det forhåndslagrede sett med attributter. Signeringsanordningens bruker blir da forespurt om å signere dataene på bakgrunn av de viste attributter.



Figur 5 Mottatt data sammenlignet med data i minnet



Figur 6 Eksempelnett for benyttelse av en mobilanordning for å signere data

Oppfinnelsens område

Den foreliggende oppfinnelse vedrører sammenkoblede data-anordninger, spesielt når kryptografisk signering benyttes for å oppnå kompatibilitet (non-repudiation), aksesskontroll, brukerverifisering etc.

Oppfinnelsens bakgrunn

Mange type applikasjoner, for eksempel e-commerce eller m-commerce, krever muligheten til å skaffe til veie varig bevis på at noen har autorisert en transaksjon. Det forventes også at signering av elektronisk materiale, slik som avtaler, forretningsrapporter og forskjellige typer skjemaer blir vanlig i nær fremtid.

E-commerce og m-commerce er stadig voksende forretningsområder, og både offentlige og private administrasjoner ser nå ut til å gjøre de tilpasninger som skal til for å åpne for elektronisk signering. Et gjennombrudd for elektronisk signering er imidlertid avhengig av sikre, motstandsdyktige og enkle prosedyrer og løsninger. Den signerende part må være sikker på at det han/hun signerer er det samme som mottas hos den mottagende part. Den mottagende part må være sikker på at den signerende part er den hun/han utgir seg for å være. Videre bør signeringen være enkel uten at det kreves noen teknisk kunnskap fra brukeren, og bør fortrinnsvis være mulig å gjennomføre uavhengig av tid og sted.

Kryptografiske signaturer blir benyttet på en rekke områder. Dette involverer typisk i tillegg til brukeren, være seg eieren av den kryptografiske signeringsanordning, et signaturbenyttende system og et signaturmottagende system. Det signaturbenyttende system spør brukeren om å legge på en kryptografisk signatur på dataene som presenteres. Brukeren signerer og returnerer signaturen tilbake til det signaturbenyttende system. Det signaturbenyttende system

kan overføre dataene som ble signert og signaturen til det signaturmottagende system. Det signaturmottagende system er en kryptografisk bindingsrelasjon mellom hva det signaturbenyttende system presenterte til brukeren for signering og hva brukeren faktisk signerte.

PKI (Public Key Infrastructure) er et mye benyttet system for krypterisk signering og autentifisering, som er velkjent for fagfolk på området. En betrodd part i et PKI-system utsteder elektroniske nøkkelpar. Paret består av en privat nøkkel og en offentlig nøkkel. Den private nøkkelen er bare kjent for brukeren (eller brukerens signeringsanordning), men den offentlige nøkkel kan være kjent for en hvilken som helst annen part som skal motta signert data fra en bruker. I brukerens anordning er objektet som skal signeres og den private nøkkel input til en eller annen algoritme som gir ut objektet i signert tilstand. Ved den mottagende part er det signerte objekt og den offentlige nøkkel input til en annen algoritme, som trekker ut det opprinnelige objektet fra det signerte objektet. Objektet vil bli trukket ut riktig kun hvis det var den korresponderende private nøkkelen som signerte det. Følgelig kan den mottagende part være sikker på at objektet ble signert av den bestemte bruker når denne brukers offentlige nøkkel benyttes for å trekke ut det opprinnelige objekt fra det signerte objekt.

Mange elektroniske anordninger støtter allerede kryptografisk signering. Et eksempel er en PC med en internettbrowser installert. Browseren kan ha én eller flere sertifikater som inneholder offentlige nøkler utstedt fra én eller flere betrodde parter eller såkalte sertifikatautoriteter (CA).

Et problem med dette er at en PC vanligvis er bundet til en fast plassering og/eller er for stor til å kunne bli båret rundt overalt. Behovet for å signere materiale er

imidlertid ikke begrenset til steder hvor PC-er er plassert eller kan medbringes.

Videre er en PC som er online til enhver tid eller for lengre perioder svært sårbar for dataspionering, og det kan være en risiko for at inntrengere får tak i de private nøklene. Av sikkerhetshensyn kan bruker komme til å ønske å benytte hans/hennes personlige signeringsanordning for å signere materiale presentert på PC-en.

Løsningen på de ovenfor nevnte problemer kan være små portable anordninger, slik som mobiltelefoner. "WMLScript Language Specification", WAP Forum, beskriver en implementering av en funksjon som gjør det mulig for WAP-telefoner å gjennomføre kryptografisk signering. WAP-telefonen spør brukeren om å signere en tekststreng ved å taste inn for eksempel en PIN-kode i anordningen for kryptografisk signering av strengen.

Slike anordninger, for eksempel mobiltelefoner, er imidlertid karakterisert ved at de er minne- og prosesseringskapasitetsbegrenset, og den kryptografiske signeringsfunksjonen er tilgjengelig gjennom et definert og begrenset grensesnitt.

Problemet oppstår da når dataene som skal signeres er for store til å bli presentert for brukeren, eller i et format som ikke er forståelig for brukeren. Dataene vil opptre som tilfeldig valgte bytes, og kan rett og slett bli oversett, og eieren av en slik anordning vil ikke være i stand til å forstå hva som skal signeres, og vil ikke få noen følelse av det som ble signert faktisk var det som skulle signeres.

Eksisterende løsninger adresserer ikke aspektet med at brukeren skal være i stand til å forstå innholdet som skal signeres som en del av signeringsprosessen i anordningen beskrevet i dette dokument.

Oppsummering av oppfinnelsen

Hovedformålet med den foreliggende oppfinnelse er å overvinne de ovenfor nevnte problemer og tilveiebringe kompatibilitet mellom en bruker, et signaturbenyttende system og et signaturmottagende system. Dette oppnås gjennom en fremgangsmåte definert av det vedlagte krav 1.

Nærmere bestemt tilveiebringer en foretrukket utførelse av den foreliggende oppfinnelse en fremgangsmåte for elektronisk og/eller digital signering av data ved å benytte en signeringsanordning og utnytte et elektronisk signeringssystem, metoden omfatter en sammenligning av dataene som skal signeres med ett eller flere attributtsett forhåndslagret i signeringsanordningen og å vise attributtene på nevnte signeringsanordning hvis nevnte data matcher alle, en del eller deler av de forhåndslagrede attributter i attributtsettet. Signeringsanordningens bruker blir da forespurt om å signere dataene på bakgrunn av de viste attributter, og den resulterende signatur returneres til signaturbrukersystemet.

Kort beskrivelse av tegningene

Figur 1 viser et eksempel på attributtsett som skal forhåndslastes i anordningen i henhold til den foreliggende oppfinnelse.

Figur 2 illustrerer et eksempel på en eier av en kryptografisk mobil anordning som benytter anordningens tastatur for å preprogrammere anordningen.

Figur 3 illustrerer et eksempel på en eier av en kryptografisk mobil anordning som benytter et programmeringsverktøy for å preprogrammere anordningen.

Figur 4 illustrerer prosedyren med å laste dataene som skal signeres i henhold til den foreliggende oppfinnelse.

Figur 5 er et flytskjema som viser dataflyten når dataene sammenlignes i signeringsanordningen i henhold til den foreliggende oppfinnelse.

Figur 6 viser et eksempelnett i hvilket en mobil anordning for signering av data benyttes.

Figur 7 viser et eksempel på signering av et dokument på en mobiltelefon i henhold til den foreliggende oppfinnelse.

Figur 8 viser et eksempel på signering av en værmelding på en mobiltelefon i henhold til den foreliggende oppfinnelse.

Foretrukne utførelser av den foreliggende oppfinnelse

I det følgende beskrives en foretrukket utførelse av den foreliggende oppfinnelse. Legg merke til at denne utførelsen diskuteres kun av illustrasjonshensyn, og begrenser ikke oppfinnelsen slik den er definert i det vedlagte krav 1.

Utførelsen som er beskrevet, tilveiebringer en fleksibel måte å gjennomføre kryptografisk binding mellom en bruker og et datasett som er ulesbart for mennesker i sin originale form, eller ikke kan presenteres i kryptografianordningen pga. datastørrelse eller dataformat.

I henhold til den foreliggende oppfinnelse, når det kreves en signatur fra personen som er i besittelse av den beskrevne anordning, må eieren ha forhåndsinnlastet informasjon som nevnte anordning kan sammenligne data som skal signeres med. Informasjon er fortrinnsvis i form av sett bitmønstre, heretter referert til som attributter, som vist i figur 1. Attributtene kan for eksempel være ASCII-representasjoner med tekstuell informasjon tilpasset til å kunne bli vist på anordningen. Et hvilket som helst antall

sett kan være definert, og hvert sett kan ha en flerhet av attributter.

Denne informasjonen lastes inn i anordningens minne ved å benytte for eksempel et programmeringsverktøy (figur 3), gjennom anordningens tastatur (figur 2) eller gjennom en eller annen prosess hvor data lastes inn i anordningens minne. Anordningens eier verifiserer denne informasjonen for eksempel ved å se gjennom dataene i minnet. Når informasjonen har blitt godkjent må en eller annen form for identifikasjon av de godkjente data bli lagret for å hindre at dataene blir modifisert. En typisk identifikator vil være dataenes kryptografiske hash.

Ved generering av en signeringsforespørsel, sender et signaturbenyttende system dataene som skal signeres til anordningen, og instruerer anordningen til å utføre en kryptografisk signering. Det signaturbenyttende system kan være et hvilket som helst datasystem, node eller datamaskin som er i besittelse av alle dataene som skal signeres. For eksempel kan det signaturbenyttende system være brukerens PC som har mottatt et eller annet skjema som krever en signatur.

Anordningen forsøker da å matche den mottatte datastrukturen som skal signeres mot attributtsett lagret i anordningen. Hvis en match er funnet, viser anordningen attributtsettet og spør om eieren ønsker å fortsette å behandle signeringsforespørselen. Anordningen viser de aktuelle data og spør eieren om å taste inn signerings PIN-koden. Anordningen signerer datastrukturen og returnerer signaturen til det signaturbenyttende system.

De opprinnelige data, eller en referanse til dem, sammen med signaturen, overføres til det signaturmottagende system. Det signaturmottagende system kan for eksempel være et permanent lager som benytter for eksempel HTTP [HTTP], LDAP [LDAP], SQL [SQL], en tidsstemplingsserver [TSP], en

eller annen form for digital offentlig tjeneste, aksesskontrollserver, transaksjonsbehandler, PKI- [PKI] basert betalingstilrettelegger eller for eksempel en småbeløpsbetalingsserver.

Forespørselen kan for eksempel sendes til anordningen som en beskyttet forespørsel som benytter en SIM Application Toolkit- (SAT) applikasjon [SAT] eller som et WML-script med en signText () forespørsel.

Figur 8 illustrerer et eksempel på en signeringsprosedyre i henhold til den foreliggende oppfinnelse. Et værvarsel skal signeres av en meteorolog ved å benytte hans/hennes personlige kryptografiske mobilanordning til å signere værmeldingen før den blir lagret på filserveren. Mobilanordningen har blitt programmert til å se etter bestemte data som spesifisert i attributtsettet. Anordningen viser attributtene. I dette tilfellet viser anordningen også de syv bytene som følger datoattributten. <attr val 7 bytes> taggen instruerer anordningen om å behandle bytene umiddelbart etter datobytemønsteret spesifisert med <attr = Date>, som ASCII-tegn for dermed å gjøre det mulig å også vise noe dynamisk innhold på anordningen.

Hovedfordelen ved den foreliggende oppfinnelse er at den gjør brukeren i stand til å forstå hva hun/han signerer, selv på små anordninger. Brukeren vet at essensiell informasjon i signeringsforespørselen er riktig før dataene signeres. Alle data som kan sendes til anordningen/signeres i anordningen, kan forstås og verifiseres av brukeren før signatur påføres. Den foreliggende oppfinnelse øker en signerende parts bevegelsesfrihet, da hun/han kan benytte portable kryptografianordninger selv for varierende datatyper.

En annen fordel ved den foreliggende oppfinnelse er at den holder brukerens private nøkkel atskilt fra det signaturbenyttende system til hvilket generelle eksterne nett er

koblet (for eksempel PC-er til Internett). Risikoen for at inntrengere kan skaffe signeringsnøklene er følgelig redusert.

Enda en annen fordel ved den foreliggende oppfinnelse er at minimale justeringer i det signaturbenyttende system er påkrevd. Oppfinnelsen i sin enkleste form kan overføre data som skal signeres til signeringsanordningen uendret, mens signeringsanordningen tar hånd om sammenligningen og uttrekningen av data som skal vises for brukeren.

Den foreliggende oppfinnelse er nå blitt beskrevet ved hjelp av bestemte eksempler. Andre utførelser som er brukbare i et hvilket som helst scenario hvor data må signeres og forstås av et menneske som benytter en liten kryptografianordning, faller innenfor oppfinnelsens rekkevidde slik den er definert i det påfølgende selvstendige krav.

Referanser

[PKCS#1] RSA Cryptography Standard
http://www.rsasecurity.com/rsalabs/pkcs/

[PKCS#7] Cryptographic Message Syntax Standard
http://www.rsasecurity.com/rsalabs/pkcs/

[WAPArch] "WAP Architecture Specification"
http://www.wapforum.org/what/technical.htm

[WML] "Wireless Markup Language", WAP Forum
http://www.wapforum.org/what/technical.htm

[WMLScript] "WMLScript Language Specification", WAP Forum
http://www.wapforum.org/what/technical.htm

[WMLCrypto] "WMLScript Crypto Library Specification", WAP Forum
http://www.wapforum.org/what/technical.htm

[HTTP] HyperText Transfer Protocol
RFC 2069
http://www.ietf.org/rfc/rfc2068

[LDAP] Lightweight Directory Access Protocol
RFC 2559
http://www.ietf.org/rfc/rfc2559

[SQL] Structured Query Language
http://www.sql.org

P a t e n t k r a v

1. Fremgangsmåte for elektronisk og/eller digital signering av et dataobjekt ved benyttelse av en signeringsanordning som benytter et elektronisk signeringssystem, k a r a k t e r i s e r t v e d

å sammenligne en forhåndsdefinert del av nevnte dataobjekt som blir trukket ut fra dataobjektet i signeringsanordningen med et sett med attributter, definert som et sett med for et menneske gjenkjennbare kodemønstre, f.eks. tekst, forhåndslagret på nevnte signeringsanordning,

å vise hele eller deler av nevnte sett med attributter på nevnte signeringsanordning hvis nevnte del av dataobjektet matcher det forhåndslagrede sett med attributter,

å forespørre en bruker av signeringsanordningen om å gjennomføre en kryptografisk signering av nevnte dataobjekt ved å benytte nevnte elektroniske signeringssystem etter å ha godkjent det/de viste hele eller deler av nevnte sett med attributter.

2. Fremgangsmåte i henhold til krav 1, k a r a k t e r i s e r t v e d at ett eller flere av attributtene inneholder dynamiske data.

3. Fremgangsmåte i henhold til krav 1 eller 2, k a r a k t e r i s e r t v e d at nevnte signeringsforespørsel sendes til signeringsanordningen som en forespørsel som benytter en SIM Application Toolkit- (SAT) applikasjon eller som et WML-script med en signText- () forespørsel.

4. Fremgangsmåte i henhold til kravene 1 - 3, k a r a k t e r i s e r t v e d de følgende trinn før sammenligningstrinnet:

i et signaturbenyttende system, å kompilere nevnte dataobjekt slik at det er kompatibelt med signeringsanordningen,

å overføre nevnte kompilerte dataobjekt til nevnte signeringsanordning.

5. Fremgangsmåte i henhold til krav 4, k a r a k t e r i s e r t v e d følgende trinn etter forespørselstrinnet:

å returnere en signatur som et resultat av nevnte signering, til nevnte signaturbenyttende system.

6. Fremgangsmåte i henhold til krav 4 eller 5, k a r a k t e r i s e r t v e d at signeringsanordningen er en liten kryptografitilpasset anordning som benytter en bestemt protokoll og at det signaturbenyttende system er tilpasset til å kompilere nevnte del av dataobjektet til nevnte protokoll.

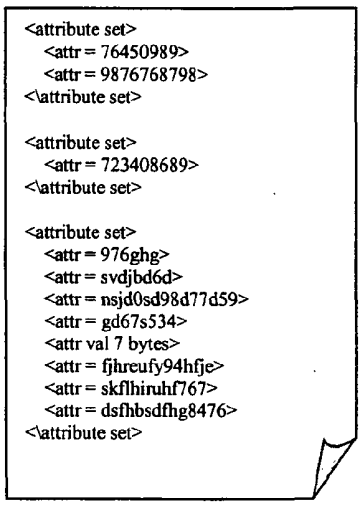
7. Fremgangsmåte i henhold til krav 6, k a r a k t e r i s e r t v e d at nevnte protokoll er WAP (Wireless Application Protocol) og signeringsanordningen er en WAP-telefon.

8. Fremgangsmåte i henhold til et av de foregående krav, k a r a k t e r i s e r t v e d at nevnte elektroniske signeringssystem benytter et privat/offentlig nøkkelpar.

9. Fremgangsmåte i henhold til et av de foregående krav, k a r a k t e r i s e r t v e d at nevnte data er et dokument, et skjema, en avtale, en transaksjon eller en PKI- (Public Key Infrastructure) sertifikatforespørsel.

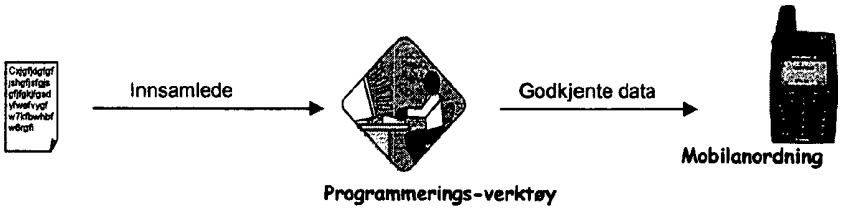
10. Fremgangsmåte i henhold til kravene 7-9, k a r a k t e r i s e r t v e d signeringen gjennomføres ved hjelp av WAP 1.2 signText- () funksjonalitet.

11. Fremgangsmåte i henhold til kravene 7-9, k a r a k t e r i s e r t v e d at signeringen gjennomføres ved hjelp av en kryptografisk signeringsapplikasjon implementert ved bruk av SIM Application Toolkit (SAT).

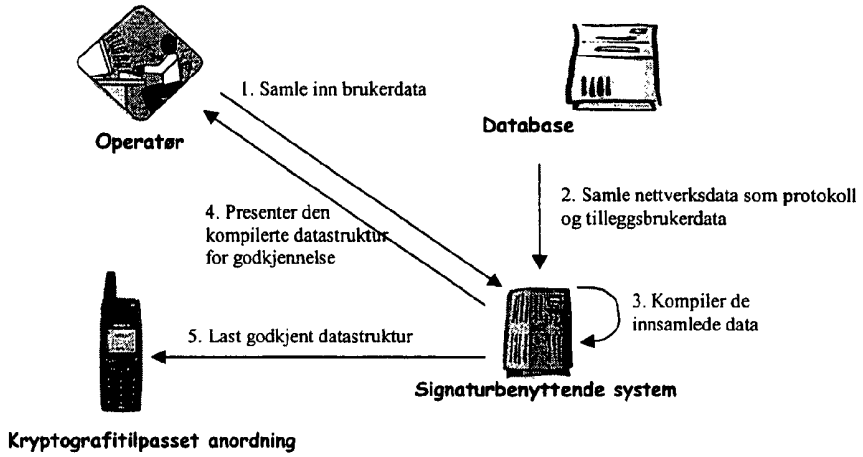


Figur 1 Eksempel på et datasett som skal forhåndslastes i anordningen.

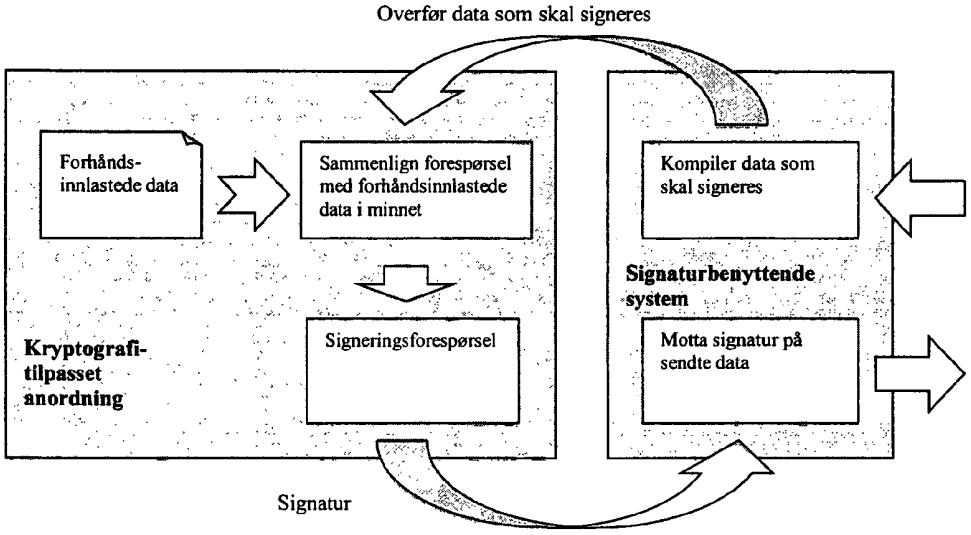
Figur 2 Eksempel på en operatør som benytter anordningens tastatur til å preprogrammere en kryptografitilpasset anordning.



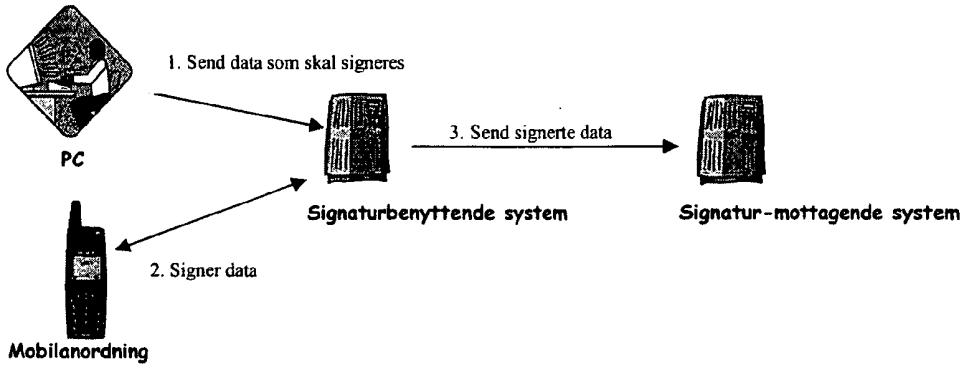
Figur 3 Eksempel på en operatør som benytter et programmeringsverktøy til å forhåndsprogrammere en kryptografitilpasset mobilanordning.



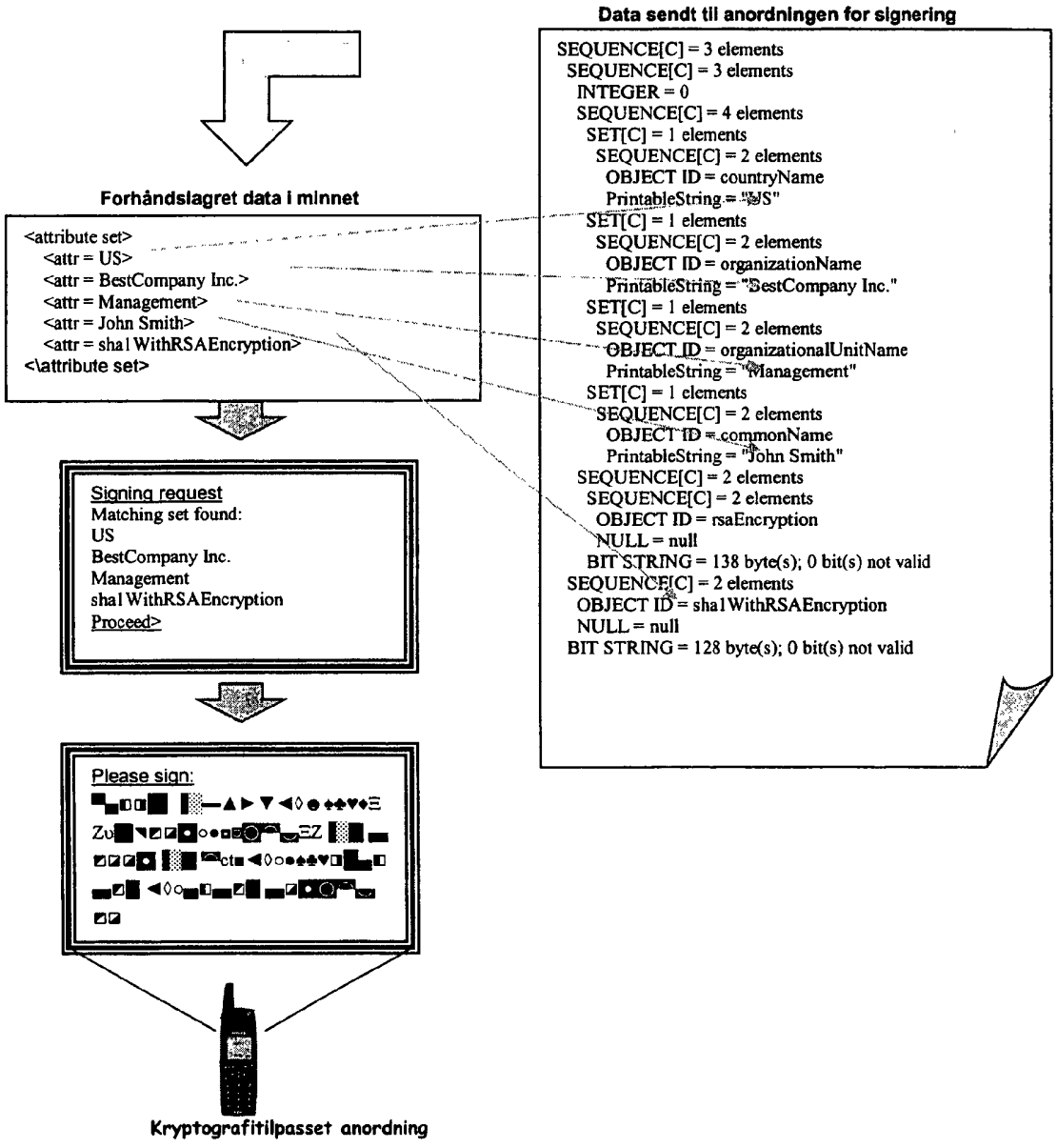
Figur 4 Forhåndsinnlasting av data som skal signeres



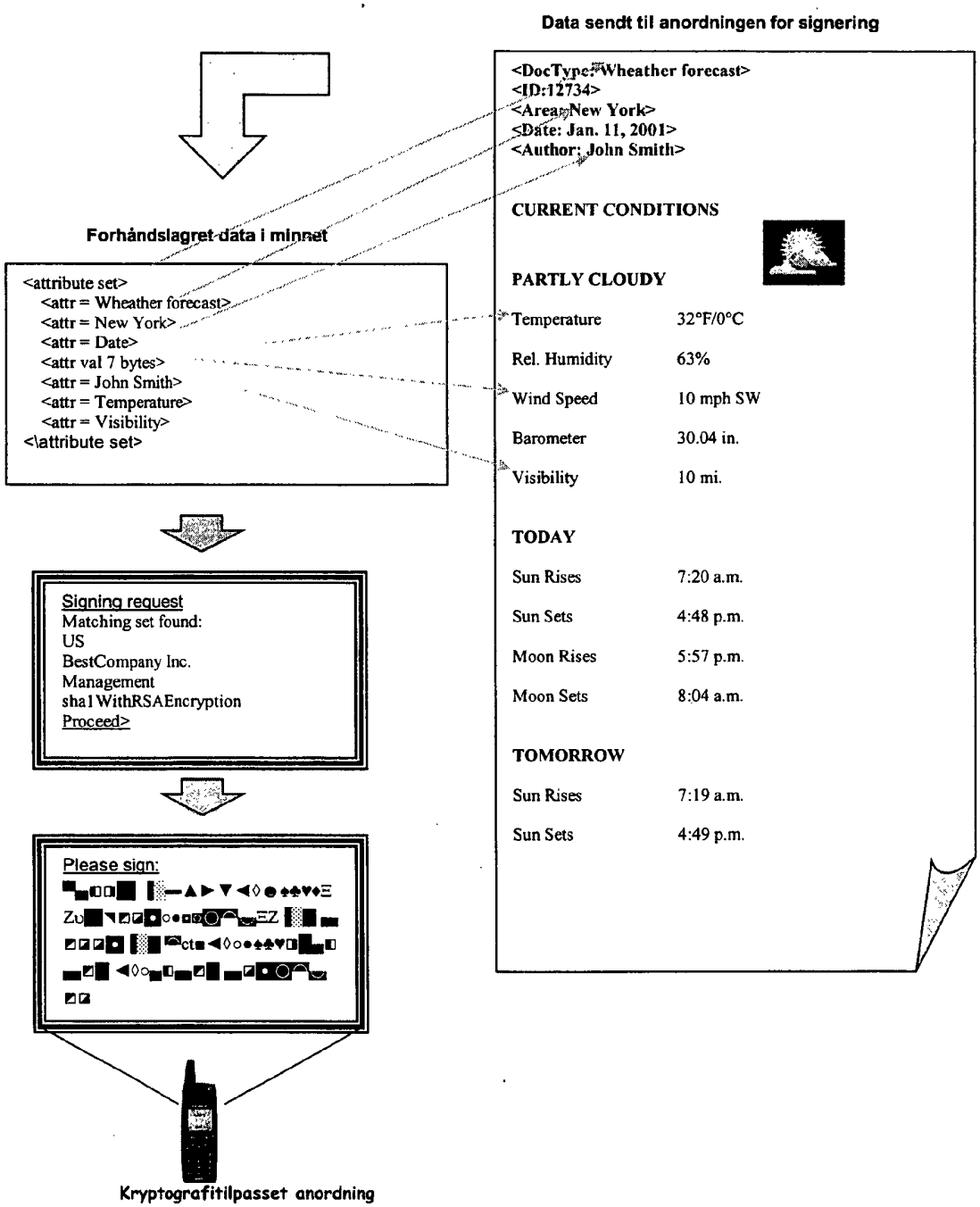
Figur 5 Mottatt data sammenlignet med data i minnet



Figur 6 Eksempelnett for benyttelse av en mobilanordning for å signere data



Figur 7 Eksempel på å signere et dokument med en mobiltelefon



Figur 8 Eksempel på å signere et dokument med mobiltelefon